UNITED STATES DISTRICT COURT

for the
District of South Dakota

IN THE MATTER OF THE SEARCH OF:

The content of the encrypted compressed storage file containing the search warrant production of Facebook User Account: FOLLOWING FACEBOOK USER: Kristy Smith; ESP User ID: 100004322865534 Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534 downloaded and currently in the possession of ICAC

Case No. 5:20-mj-87

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251, 2252, 2252A	Production, Receipt, and Possession of Child Pornography

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Affiant Signature

Sarah B. Collins, Assistant U.S. Attorney
Printed Name and Title

Sworn to before me and:
☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 4/15/2020

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:
The content of the encrypted compressed storage file containing the search warrant production of Facebook User Account: FOLLOWING FACEBOOK USER: Kristy Smith; ESP User ID: 100004322865534 Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534 downloaded and currently in the possession of ICAC

Case No. 5:20-mj-87

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota *(identify the person or describe the property to be searched and give its location)*:

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, 2252A, as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before April 29, 2020 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)*. ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 4/15/2020 3:40pm

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

cc: AUSA Collins

Return

Case No.: 5:20-mj-87	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF:
The content of the encrypted compressed storage file containing the search warrant production of Facebook User Account: FOLLOWING FACEBOOK USER: Kristy Smith; ESP User ID: 100004322865534
Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534
downloaded and currently in the possession of ICAC

5:20-mj-87

SEALED

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

I, Elliott Harding, Rapid City Police Department Detective and currently assigned to the South Dakota Internet Crimes Against Children Taskforce (ICAC), being duly sworn, states as follows:

1. I have been a law enforcement officer since December 1, 2008. I have received training at the Law Enforcement Training Academy in Pierre, SD, training as a new police officer recruit along with various Police Training Officers and my own experience working in the Patrol Division. I have worked as a Detective in the Criminal Investigations Department beginning April of 2014 and primarily focused on stolen vehicles, pursuits and other general property crimes. During that time, I attended the Reid Technique of Interview and Interrogations. I have worked as a Detective in the Internet Crimes Against

Children (ICAC) Task Force since August of 2015. During this time, I have attended classes in regards to on-line ads and undercover chat investigations as it pertains to child exploitation as well as prostitution/human trafficking. I have also attended classes in regards to the BitTorrent Network as it pertains to the download and sharing of child pornography files. As a Special Assistant Attorney General with State of South Dakota my duties include investigations related to illegal possession and distribution of images containing sexually explicit material, and investigations dealing with illegal activities concerning the Internet or World Wide Web.

2. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statues 18 U.S.C. §§ 2251, 2252 and 2252A, involving violations of law involving child pornography. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I have been informed that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the manufacture, distribution, receipt and possession of child pornography.

4. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law

enforcement officers, interviews of persons with knowledge, my review of documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not withheld information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. Your affiant respectfully submits that there is probable cause to believe that Karl Koster committed the crimes of distribution, receipt and possession of child pornography in violation of 18 U.S.C. § 2252 and 2252A, and evidence is present in the search warrant production for following Facebook account (also referred to as SUBJECT CONTENT) USER: Kristy Smith; ESP User ID: 100004322865534, Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534.

6. There is also probable cause to search the information described in Attachment A for evidence, contraband, or fruits of these crimes, as further described in Attachment B. Specifically, there is probable cause that evidence of those crimes will be found in the content of the encrypted compressed storage file provided to me on Facebook's law enforcement portal in response to a previous search warrant obtained on March 4, 2020. Facebook provided the content on March 23, 2020,

beyond the 14-day limit on the previous warrant. I thereafter downloaded the file, but did not review the contents of the file, nor did I provide access to the file for anyone else to view. I did view the PDF version to ensure the download properly occurred. The downloaded file is currently in the possession of ICAC.

7. It is my understanding that I must seek this additional warrant to review the responsive materials out of an abundance of caution to comply with the issue raised in dicta in the recent decision in *United States v. Nyah*, 928 F.3d 694 (8th Cir. 2019).

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the

visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud-based storage service," as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic,
optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in

conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. "Electronic Storage Device" includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking

and/or internet access capabilities, and any "cloud" storage by any provider.

l. "Encrypted compressed storage file" as used herein, refers to a computer file whose contents of one or more files are compressed for storage or transmission, one example is a "zip file." The compressed storage file is used to large files or multiple files into one file for ease of transfer. The ESPs create the file then provide access to the file to law enforcement typically via the ESP's law enforcement portal.

m. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for

their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

p. "PhotoDNA" is a process where a photograph is scanned by converting images into a grayscale format, creating a grid and assigning a numerical value to each tiny square. Those numerical values represent the "hash" of an image, or its "PhotoDNA signature." The program protects user privacy in that it doesn't look at images or scan photos; it simply matches a numerical hash against a database of known illegal images. A hash is an alphanumeric value assigned to an image based off a mathematical algorithm run against the data making up the file itself. This process has proven to be a reliable method of confirming like images.

q. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell

phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

u. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

v. "Zip file," as used herein is a type of "Encrypted compressed storage file," defined above in paragraph l.

BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

b. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can

save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

e. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can

set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user's computer or external media in most cases.

10. From my training and experience, I am aware that when Electronic Service Providers, like Facebook, provide access to an encrypted compressed storage file, typically a zip file, on its law enforcement portal. The link is to a file that is limited to the content of the account authorized by the search warrant and no other accounts.

PROBABLE CAUSE

11. On January 7, 2020, I received CyberTips 60983628 and 61155796 from the National Center for Missing and Exploited Children (NCMEC). The reporting parties were Facebook and Yahoo respectively. The CyberTips were copied to compact disc under this case report number and stored in ICAC evidence. Below is a brief summary of the information.

CYBERTIP 60983628

12. The cybertip contained the following information:

- Reporting ESP: Facebook
- **Incident Information**
  - Incident Type: Child Pornography (possession, manufacture, and distribution)
  - Incident Time: 12-10-2019 04:58:17 UTC
- **Suspect**
  - Name: Karl Koster
  - Mobile Phone: +16058582472 (Verified)
  - Date of Birth: 09-18-1981 Approximate Age: 38
  - Email Address: kosterkarl@yahoo.com (Verified)
  - Screen/User Name: karl.koster.75 ESP User ID: 100002462616167

  - Profile URL: http://www.facebook.com/karl.koster.75
  - IP Address: 2600:1014:b06f:c42c:1938:d518:bd08:214f (Login)
  - 11-30-2019 03:30:16 UTC
  - IP Address: 67.158.42.135 (Other)
  - 12-10-2019 03:57:24 UTC
- Additional Information: Estimated location on December 11, 2019 UTC: Deadwood, South Dakota, US (Not Verified) Email: kosterkarl@yahoo.com (Verified)
- This report contains a recent, believed-to-be non-mobile IP address under event type Other.
- **Additional Information Submitted by the Reporting ESP**
  - This report contains additional information about the recipient of the reported content:
  - Recipient(s):
    - First Name: Kristy
    - Last Name: Smith
    - Email: kosterkristy1@gmail.com (Verified)
    - Age: 28
    - DOB: 1991-09-18
    - Gender: Female
    - Profile Url: http://www.facebook.com/people/Kristy-Smith/100004322865534 **(SUBJECT CONTENT)**
    - Account ID: 100004322865534
    - IP Address: 67.158.42.135
    - IP Capture Date: December 10, 2019 at 05:23:38 UTC
- **Uploaded File Information**
  - Number of uploaded files: 2
  - Filename: 73bffa4tjhs8c8cc79222830_426638568004705_2097147065082576896_n .jpg
  - MD5: 60f74a6fc39786d984dea0e5e5e9687b
  - Submittal ID: 07911e343617de923cb5df9c03abcd36
- Did Reporting ESP view entire contents of uploaded file? Yes
- Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
- Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
- Sent in product: Messenger
- File's unique ESP Identifier: 426638564671372
- Uploaded December 10, 2019 at 04:58:17 UTC
- Type: IP Address
- Value: 67.158.42.135
- Event: Upload

- Date/Time: 12-10-2019 04:58:17 UTC
- **Uploaded File Information**
  - Filename: 83v5mpsdzkkc008s67763403_2359381157487282_5293448283518140416_n.jpg
  - MD5: 441a3321504923412 45bec02d7f87990
  - Submittal ID: b44535ee82a31bf407749f15fc1f6a57
  - Did Reporting ESP view entire contents of uploaded file? Yes
  - Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
  - Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
  - Additional Information: This is the profile picture for the account 10000246261616

PHOTO OBSERVATIONS FOR CYBERTIP 60983628

13. I observed 73bffa4tjhs8c8cc79222830_42663856800 4705_ 2097147065082576896_n.jpg. The photo showed a girl approximately 9-11 years of age with blond hair. The girl was wearing red, long sleeved shirt, white shoes, gray socks, white and gray undershirt and no pants. The girl's nude vagina was exposed. The girl's hands and torso were tied with white rope which was suspended above her. The girl appeared to be in a storage room of some type. One box in the storage area appeared to have JAAR-MARKT written on it. In the top left corner, I could see manfredo.fotoplenka.ru, written on the photo.

14. I observed 83v5mpsdzkkc008s67763403_2359381157487282_ 529 3448283518140416_n.jpg. The photo showed a dark colored pickup truck parked outside. Detective Jeremy Stauffacher informed me he had seen the same picture on a cell phone he examined belonging to Karl Koster (9/18/81) during a prior investigation, described below.

CYBERTIP 61155796

15. Information contained in this cybertip is as follows:

- **Reporting Electronic Service Provider (ESP):** Yahoo! Inc
- **Incident Information**
  - Incident Type: Child Pornography (possession, manufacture, and distribution)
    Incident Time: 12-13-2019 15:00:12 UTC
    Description of Incident Time: This is the date/time when Oath submitted the CyberTip to NCMEC.
  - **Suspect**
    - Name: Karl Koster
      Phone: 1 6054841348
      Email Address: kosterkarl@yahoo.com
      ESP User ID: 4YJ5HLBMKTYVGXEJTRCKNZ7RFE-yahoo
      Additional Information: Alternate Email: kosterkristy1@gmail.com
- **Additional Information Submitted by the Reporting ESP**
  - Platform: Files were transmitted over Yahoo Mail.
    Offense date: 2019/12/12 - 16:34:15
    Recently used IP: 67.158.42.135/2019/12/12 - 16:34:15
- **Uploaded File Information** (image one of four)
  - Number of uploaded files: 4
  - Filename: image.5-1.png
  - MD5: 730a1e1965d393284be5306ea3569d5e
    Submittal ID: b3e585d883348c0bb17c5a0530863da8
    Original Filename Associated with File: 15760632237637659062 86.jpg
    Did Reporting ESP view entire contents of uploaded file? Yes
    Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
    Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
    Additional Information: message ID for this upload: AC89A2FQBoMnXfDRMgro-JyHKg8
  - Additional Information: Upload Date/Time: 2019-12-11 11:21:22
- **Uploaded File Information (image two of four)**
  - Filename: image.6-1.png
  - MD5: 730a1e1965d393284be5306ea3569d5e
    Submittal ID: 00280c22ec583b5d87967041024596a3
    Original Filename Associated with File: 15760632237637659062 86.jpg

Did Reporting ESP view entire contents of uploaded file? Yes
Did Reporting ESP view the EXIF of uploaded file?
(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?
(Information Not Provided by Company)
Additional Information: message ID for this upload:
ACBVwotDY68WXfDRKwa6qOWHokM

- Additional Information: Upload Date/Time: 2019-12-11 11:21:14

- **Uploaded File Information (image 3 of 4)**
  - Filename: image.7-1.png
  - MD5: 0a6dea3ce4a274b5b7af3f0fe0722fb2
    Submittal ID: 30d80463f59e21424ebcb313dcb00d48
  - Original Filename Associated with File:
    15760626929362053990695.jpg
    Did Reporting ESP view entire contents of uploaded file? Yes
    Did Reporting ESP view the EXIF of uploaded file?
    (Information Not Provided by Company)
    Were entire contents of uploaded file publicly available?
    (Information Not Provided by Company)
    Additional Information: message ID for this upload:
    ALqcJkB9r5iUXfDPHQ5T-KrSlRo
  - Additional Information: Upload Date/Time: 2019-12-11 11:12:29
- **Uploaded File Information (image 4 of 4)**
  - Filename: image.8-1.png
  - MD5: 0a6dea3ce4a274b5b7af3f0fe0722fb2
    Submittal ID: 4f7a4e1b8b9eec91f19f39243602bc66
    Original Filename Associated with File:
    15760626929362053990695.jpg
    Did Reporting ESP view entire contents of uploaded file? Yes
    Did Reporting ESP view the EXIF of uploaded file?
    (Information Not Provided by Company)
    Were entire contents of uploaded file publicly available?
    (Information Not Provided by Company)
    Additional Information: message ID for this upload:
    AGXgs0soG1oUXfDPFg2I2HVK-8o
  - Additional Information: Upload Date/Time: 2019-12-11 11:12:22

PHOTO OBSERVATIONS FOR CYBERTIP 61155796

16. I observed image.5-1.png and image.6-1.png. Both images appeared to be duplicates of each other. The picture showed a girl approximately

5-8 years of age with shoulder length dark hair. The girl wore only silver colored sandals. I could the girls nude breast area and nude vagina. The girl was standing in a wooded area. The girl was holding a pair of white underwear with an unknown design. The top left of the picture showed the icon of what appeared to be a nude female of unknown age with the text "ONLINE-LOLITA.com" written underneath the icon.

17. I observed image.7-1.png and image.8-1.png. Both images appeared to be duplicates of each other. The picture showed a girl approximately 5-8 years of age with shoulder length dark hair. The girl was kneeling on a bed with a brown zebra stripe pattern. The girl was smiling at the camera. I could see the girl's nude breast area and nude vagina. In the background, I could see a red stuffed animal which appeared to be a bird. Other stuffed animals could be seen behind the girl, but I could not determine what they were. The headboard of the bed was tan in color.

IDENTIFYING KARL KOSTER

18. Local police records showed a Karl Koster (9/18/81) living at 314 Summit St. #70, Belle Fourche, SD. Local records showed Karl's phone number as 605-858-2472 as of 11/18/19. It should be noted the name, date of birth and phone number in local records matched those listed in the suspect information under CyberTip 60983628.

19. Local records also showed Karl to have the phone number 605-484-1384 as of 1/16/19. This phone number is very similar to the phone number of the suspect provided in CyberTip 61155796 which is 605-484-1348.

20. CyberTip 60983628 described Karl Koster sending, child pornography to Kristy Smith via Facebook Messenger. The CyberTip noted Kristy's email address as kosterkristy1@gmail.com and Kristy's date of birth as 9/18/91. Kristy's date of birth is the same as Karl's, but 10 years younger. Detective Stauffacher informed me he had observed pictures of Karl wearing what appeared to be woman's underwear, in a prior investigation described in paragraph 17. I believe Kristy Smith is Karl Koster. Persons engaging in child pornography crimes often send themselves the illicit images utilizing multiple accounts, particularly if he believes his identity is obscured in an account that does not link to his legal name.

21. Koster was previously convicted in Pennington County, South Dakota, for Make/Sale/Posses Child pornography and was sentenced on January 3, 2005 to 5 years' imprisonment on three counts to be served consecutively. He paroled in December, 2010 and has remained on parole since that date.

22. In October 2019, South Dakota State Parole Agent GP Carmichael brought a phone to ICAC and asked that ICAC forensically examine the device. Agent Carmichael indicated the phone belonged to a parolee, Karl Koster. Carmichael indicated that Koster was on parole for a previous conviction for state child pornography charges. Det. Jeremy Stauffacher conducted an examination in CR: 19-108287. Though he did not find child pornography, he did locate images of young girls and concerning Google searches like, "girls in panties," as well as the identifying images described above in paragraph 15.

23. On February 11, 2020, Parole Officer Jennifer Leighty contacted Det. Stauffacher about examining additional devices. She told him that she was conducting a parole search at the time on Karl Koster and that Koster had been placed in jail on a parole hold. Stauffacher informed Leighty of the ICAC investigation into Koster related to the above-described cybertips and that ICAC was planning to conduct a search on Koster's residence in the near future. Leighty seized twenty-one items of evidence (the SUBJECT DEVICES) pursuant to her parole search and turned them over to ICAC. The items remain in ICAC custody awaiting this search warrant.

24. I reviewed Koster's parole agreement, which he signed on 11/18/10 and 12/1/10. In that agreement, Koster agreed that he and all of his possessions were subject to warrantless searches upon reasonable suspicion by the parole agent or other law enforcement. In the agreement, he was also prohibited from possessing internet capable devices without prior approval of parole and sex offender treatment provider. Of the devices seized by parole on February 11, 2020, multiple were internet capable.

25. I obtained a search warrant for the above-described Facebook account on March 4, 2020 and served it on Facebook the same day. March 18, 2020, was the deadline for Facebook's return of information on the warrant. Facebook failed to provide responsive data by that date, instead it provided the data to me on March 23, 2020.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS CHILD PORNOGRAPHY

26. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The user often maintains these child pornography images for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material,

and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found within the SUBJECT CONTENT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. § 2703, by using the warrant to permit access to the encrypted compressed storage file previously provided by Facebook according to a search warrant. The file is particularly described in Attachment A. Upon receipt of the warrant, the government-authorized persons will review the contents of the file to locate the items described in Section II of Attachment B.

JURISDICTION

28. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3). 18 U.S.C. § 2703. Specifically, this Court is a "district court of the United States

(including a magistrate judge of such court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

LIMIT ON SCOPE OF SEARCH

29. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

REQUEST FOR SEALING OF MATTER

30. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

CONCLUSION

31. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the encrypted compressed storage file provided by Facebook in compliance with a previous warrant, there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Facebook account, listed in Attachment A has been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of

child pornography), which items are more specifically described in Attachment B. There is probable cause to believe that Karl Koster, the likely user of the Facebook account, received and distributed child pornography with other unknown users, and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The encrypted compressed storage file is of the content of the account associated with user: USER: Kristy Smith; ESP User ID: 100004322865534, Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534.

Dated: 4/15/20

Det. Elliott Harding
Rapid City Police Department
Internet Crimes Against Children
Taskforce

Sworn to before me and:
☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

this 15th day of April, 2020

Daneta Wollmann
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the encrypted compressed storage file provided by Facebook, Menlo Park, California. The encrypted compressed storage file is of the content of the account associated with user: USER: Kristy Smith; ESP User ID: 100004322865534, Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534.

The encrypted compressed storage file has been downloaded from Facebook's law enforcement portal, but not reviewed and is in secure storage at ICAC.

ATTACHMENT B
Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information agents are authorized to search:

To the extent that the information is contained within the encrypted compressed storage file described in Attachment A, agents are hereby authorized to search the entirety of the file including all contents, including any messages, records, files, logs, or information that had been deleted but was still accessible by Facebook. And all contact and personal identifying information, including for Facebook user IDs and regarding the following account:

USER: Kristy Smith; ESP User ID: 100004322865534; Profile URL: http://www.facebook.com/people/Kristy-Smith/100004322865534.

(a) including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the accounts and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall

postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the accounts;

(h) All records of the accounts' usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the accounts are or were a "fan" of;

(j) All past and present lists of friends created by the accounts;

(k) All records of Facebook searches performed by the accounts;

(l) All information about the users' access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the accounts;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the Facebook account associated with encrypted compressed storage file for the Facebook account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, (production, receipt and possession of child pornography) including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;

b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;

c. Evidence indicating how and when the Tumblr account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the account owner or user;

e. Evidence indicating the account users or owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including

records that help reveal the whereabouts of such person(s);

g. Records relating to who created, used, or communicated with the account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram;

3. Evidence of who used, owned, or controlled the account or identifier associated with the file described in Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers associated with the file described in Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier associated with the file described in Attachment A and other associated accounts.